EXHIBIT A

From:	Krajcir, Robert [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=26414B37173741E09B795763D9ADA51D-KRAJCIR, RO]
Sent:	1/16/2020 3:28:42 PM
To:	Quitugua, Eric [o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=227693e84bc0400b84364660f692bc85-Quitugua, E]; Brown, Timothy [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=a1bcd95116e84d6692dd89f9d55c5b7a-Brown, Timo]
CC:	Pierce, Charles [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=8821c5f3c8734a3fbd33de946353d52b-Pierce, Cha]; Sejna, Tomas [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=0f1c6bd3d32f4ca0966247ae2386cc56-Sejna, Toma]
Subject:	RE: Machine certificate authentication

Hi Eric,

Regarding WiFi – implementation of Aerohive was a great help, as we are now able to force all the Android or iPhone devices to guest subnet, even though user connects with proper credentials to corporate SSID. However, we are still unable to stop users connecting to our network from unmanaged laptop with Windows or MacOS, as this works on OS detection only.

Regarding GP VPN we are still standing on the same spot. Anyone can connect from anywhere as long as they know AD credentials. I was able to at least trim access from 3rd party devices on x-auth (devices that do not support GP = Linux, Androids etc.), so that only two gateways allow this now and all the traffic from such devices is being inspected (no split-tunneling). I'd like to go even further and get this to a point where users will have to specifically ask for such access for their devices (via ticket with business reason, manager and InfoSec approval), and even this access will be restricted. While certificates would be able to solve this for us, they are useless as long as users have full admin rights (certificate can be exported and installed anywhere if user is an admin).

The best thing we can currently hope for is implementation of NAC, which would solve all these issues. We are currently talking to vendors about their solutions, will have quotes available soon. Let's hope budget will allow us to purchase such solution as planned. However, this process will get at least 6 months, if not entire year till full adoption.

Best regards,

Robert

solarwinds

Róbert Krajčír | Network Engineer
Office: +420 511 12 6277 | Cell: +420 775 395 043

From: Quitugua, Eric
Sent: Thursday, January 16, 2020 16:12
To: Brown, Timothy <timothy.brown@solarwinds.com>; Krajcir, Robert <robert.krajcir@solarwinds.com>
Cc: Pierce, Charles <charles.pierce@solarwinds.com>; Sejna, Tomas <tomas.sejna@solarwinds.com>
Subject: FW: Machine certificate authentication
Importance: High

Tim,

This was @Krajcir, Robert suggestion on how to address non-corporate machines from connecting to the network using GP VPN. As you know, this did not get any traction, but wanted to share with you so that we can circle this back and see if we can re-assess and possibly implement some type of enforcement.

@Krajcir, Robert if you have any other information you'd like to share, let's set something up and talk to Tim about some of what you described below.

-EQ

Eric Quitugua | Sr. Manager | **SolarWinds Information Security**
eric.quitugua@solarwinds.com | 512-498-6200

From: Krajcir, Robert <robert.krajcir@solarwinds.com>
Sent: Friday, August 24, 2018 4:13 AM
To: Taylor, Brody <brody.taylor@solarwinds.com>; Murray, Joe <Joe.Murray@solarwinds.com>; Henry, Jonathan <jonathan.henry@solarwinds.com>
Cc: Quitugua, Eric <eric.quitugua@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; Kenneally, Jonathan <Jonathan.Kenneally@solarwinds.com>; Straub, Carol <carol.straub@solarwinds.com>; Cline, Brad <brad.cline@solarwinds.com>; Pierce, Charles <charles.pierce@solarwinds.com>; Masar, Marek <Marek.Masar@solarwinds.com>
Subject: RE: Machine certificate authentication

Hello all,

I would like to drag your attention back to this topic.

Implementing certificates is essential to enforce proper security policies not only on VPN, but also on corporate wireless, to properly address BYOD problem. We see every day, that people are accessing our corporate wifi with their smartphones or other devices that are not joined in the domain – this seems to be common practice !!! While we do not have any control over such device (proper antivirus, NetScope, OS updates etc.), it can easily reach any resource on any port on our corporate or swdev network.

To summarize the risk we are facing:
- Anyone with AD credentials can access our corporate wifi or corporate VPN from ANY device, no matter if company owned or not
- While on corporate wifi, or VPN, such device can basically do whatever without us detecting it until it's too late:
  o It can easily download any content without being detected by NetScope, which is normally installed on all domain PCs
  o it can compromise entire network by spreading malware (spyware, viruses, trojans, ransomware), because we cannot ensure that such device will be fully compliant in terms of OS updates, antivirus, software installed etc.

I do not want to look like panicking, but I hope I do not have to explain what would be the impact on this company, if someone connects non-domain PC or phone with ransomware like WannaCry into our network. Even though we will be able to see who's AD credentials were used to access the network, it will be to very little use once we will have to deal with stolen or encrypted data or malware epidemic, especially when we know that sometimes people are leaving the company, but their AD creds remain active for few more days.

I would like to emphasize, that we need to get some solution together as soon as possible. For the one I proposed, we would need to:

- trim down user admin rights, so that they won't be able to export certificates on their PC
- enroll certificates
- set VPN and wireless policies to accept only devices with valid certificate, and with valid AD credentials

I would like to schedule a call about this with all interested parties to agree on some action plan, so that we can get things moving. Let me know if you have any questions or concerns.

Best regards,

Robert

solarwinds

Róbert Krajčír | Network Engineer
Office: +420 511 12 6277 | Cell: +420 775 395 043

From: Krajcir, Robert
Sent: Thursday, June 7, 2018 18:37
To: Taylor, Brody <brody.taylor@solarwinds.com>; Murray, Joe <Joe.Murray@solarwinds.com>; Cline, Brad <brad.cline@solarwinds.com>
Cc: Quitugua, Eric <eric.quitugua@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; Kenneally, Jonathan <Jonathan.Kenneally@solarwinds.com>; Straub, Carol <carol.straub@solarwinds.com>
Subject: RE: Machine certificate authentication on GlobalProtect VPN

Hi Brody,

That is a good question. At this moment, it seems it is everyone. Looking at the membership in AD groups, most of SWI employees can use the VPN. Yes, I believe there are groups of users who do not need access to on-premise resources at all, but I do not know how to determine which groups.

Best regards,

Robert

solarwinds

Róbert Krajčír | Network Engineer
Office: +420 511 12 6277 | Cell: +420 775 395 043

From: Taylor, Brody
Sent: Wednesday, June 6, 2018 22:55
To: Krajcir, Robert <robert.krajcir@solarwinds.com>; Murray, Joe <Joe.Murray@solarwinds.com>; Cline, Brad <brad.cline@solarwinds.com>
Cc: Quitugua, Eric <eric.quitugua@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; Kenneally, Jonathan <Jonathan.Kenneally@solarwinds.com>; Straub, Carol <carol.straub@solarwinds.com>
Subject: RE: Machine certificate authentication on GlobalProtect VPN

Dumb question, who are the user segments needing to access our domain assets post O365 / SharePoint?

solarwinds

Brody Taylor | Director ITSM & EUS | SolarWinds
Office: 512.682.9320 | Mobile: 512.652.8345

From: Krajcir, Robert
Sent: Tuesday, June 5, 2018 8:23 AM

To: Murray, Joe <Joe.Murray@solarwinds.com>; Cline, Brad <brad.cline@solarwinds.com>; IT HD Leads <ithelpdeskleads@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Quitugua, Eric <eric.quitugua@solarwinds.com>
Cc: Network Team <NetworkTeam@solarwinds.com>
Subject: RE: Machine certificate authentication on GlobalProtect VPN

Hey Joe,

Thanks for your email.

Yes, I agree that we have a lot to consider, that is why I have started this discussion at the first place. However, I would like to move our environment a bit further, as the only other option is to do nothing.

Regarding your concern – let me explain my vision a bit further. There should be two groups (or eventually more) of users:

Users accessing our VPN from company-owned device – should use machine certificate to authenticate their PC, should possess unlimited access (as if they were in the office)
Other users – should still have an option to connect to VPN, but their profile should have stricter policy and tier access should be limited. Also the number of gateways can be lower, i.e. just a few per region – Austin, Lehi/Denver, Ottawa, Cork, Brno, Manila, Singapore…
There could be also separate groups for vendors, contractors etc., depending on how many levels of restriction will be required.

So in my point of view, vendors, or non-domain computers in general should not have unrestricted access to our network, and thus should fall under one of the restricted categories that does not need any certificates. As for acquisitions – this initiative should motivate them to join tier PC to domain, especially laptops. Workstations that are always in the office do not matter, as there they are protected by our firewalls all the time. However, laptops, that can be carried away are what matters – if they are not in the domain, we cannot control their security outside of our network.

One other challenge is to issue a certificate to each machine in the domain, so it will not be exportable (user will not be able to read the private key), otherwise it would be easy to copy the certificate from one machine to other and bypass the entire idea. Question also is whether to create unique certs for each machine (i.e. bound to hostname, preferred method), or use one universal (wildcard one) and distribute everywhere.

@Tara, Marek – are we able to push certificates to machines so that users won't be able to export them / read private key? Will we need to trim user rights to achieve this?

Best regards,

Robert

solarwinds
Róbert Krajčír | Network Engineer
Office: +420 511 12 6277 | Cell: +420 775 395 043

From: Murray, Joe
Sent: Tuesday, June 5, 2018 9:28
To: Krajcir, Robert <robert.krajcir@solarwinds.com>; Cline, Brad <brad.cline@solarwinds.com>; IT HD Leads <ithelpdeskleads@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Quitugua, Eric <eric.quitugua@solarwinds.com>

Cc: Network Team <NetworkTeam@solarwinds.com>
Subject: RE: Machine certificate authentication on GlobalProtect VPN

Hi Robert,

I agree with the reasoning, however, I think it is needed as is for now.
Between vendors and all the acquisitions, we utilize VPN a lot for off domain computers (in fact they can be very reliant on it).

If Infosec would really like this looked at further, we could discuss possible ways to implement, but I think we have a lot to consider.

Note: if we did proceed, the root cert is already on all domain joined computers. It would just mean issuing a cert from our internal CA which would only take 2 minutes.

Thanks,

Joe

From: Krajcir, Robert
Sent: Monday 4 June 2018 15:49
To: Cline, Brad <brad.cline@solarwinds.com>; IT HD Leads <ithelpdeskleads@solarwinds.com>; Trebacz, Marek <Marek.Trebacz@solarwinds.com>; OConnell, Tara <Tara.OConnell@solarwinds.com>; Quitugua, Eric <eric.quitugua@solarwinds.com>
Cc: Network Team <NetworkTeam@solarwinds.com>; Murray, Joe <Joe.Murray@solarwinds.com>
Subject: Machine certificate authentication on GlobalProtect VPN

Hello all,

By this initiative, I would like to address following problem:

These days, we are in process of firewall cleanup and optimization, which showed us a security gap we are facing with our VPN service. As GlobalProtect VPN client is publicly available for download, it is no problem for almost any user to download it to any PC they like, and log in to our VPN from 3rd party device – without Netskope, proper Antivirus, security patches or updates etc. This is not only a major drawback from opening access to our network via VPN completely (as we intend to in the future, as it will be required by teleworkers, on business trips etc.), but I guess we all will also agree, that it is not very secure for resources currently accessible via VPN and data stored there, especially considering stricter legislation such as GDPR.

What I propose:

Use certificates for machine authentication. Basically it would mean, that users will only be able to connect to our VPN from verified/trusted devices, that are under IT control, joined the domain, are properly updated and have the required software properly installed and in use. For everyone else, there could be one or two separate VPN gateways per region with stricter policy (access to less resources).

What do we need:

As far as I have researched, there are no additional costs associated with implementing certificates. We do not need additional licenses or hardware. Joe also informed me, that we already have our internal CA server that can be used for this purpose. So what we need to do is basically this:
- configure new connection profiles on our firewalls,

- import root certificate on the firewall
- Issue, push and install certificates to client machines – i.e. in waves via SCCM, or let users download manually from a server accessible only from office... <mark>subject to further discussion</mark>
- Implement a pilot (i.e. all IT people as testers)
- Roll out to all users
- Create/modify the policies for access from corporate devices and from 3rd party devices

<u>The reason why I am writing this email:</u>

I would like to get inputs from you folks, especially your thoughts on the solution itself, on how exactly to push the certificates to user machines, how the support should look like, testing period etc. Feel free to comment or forward to anyone who may be interested but I accidentally omitted him/her from the recipient list.

Thank you!

Best regards,

Robert

solarwinds

Róbert Krajčír | Network Engineer
Office: +420 511 12 6277 | Cell: +420 775 395 043